UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	**No. 3:24-CR-00151**
v.	)	**JUGDE RICHARDSON**
	)	
MATTHEW ISSAC KNOOT	)	

REPLY SUPPORTING MOTION TO DISMISS

Counts 1, 4, 5, and 6 of the indictment should be dismissed because the facts alleged in support of those counts (even if true) do not state an offense. *United States v. Superior Growers Supply*, Inc., 982 F.2s 173, 177 (6th Cir. 1992) (explaining that, "[t]o be legally sufficient," an "indictment must assert facts which in law constitute an offense"); Fed. R. Crim. P. 12(b)(3)(B)(v).

Resisting this outcome, the Government generally claims that the theories of liability laid out in the indictment are legally adequate to give rise to claims for violations of (or conspiracies to violate) the computer fraud, identity theft, and unlawful-employment-of-illegal-aliens statutes.

For the reasons set forth below, however, the Government's arguments fall short. Consequently, this Court should dismiss Counts 1, 4, 5, and 6 for failure to state an offense.

A. Counts One & Four: Computer Fraud

The Government's theory for Counts One & Four is that Knoot committed or conspired to commit computer fraud in violation of 18 U.S.C. § 1030(a)(5)(A) when he installed commercially-available remote desktop applications onto computers owned by Companies A, B, C, and D because by doing so (the Government says) he enabled a third-party (Yang) to remotely logon to those computers and perform IT work for the benefit of those companies.

That theory is a non-starter. To violate or conspire to violate § 1030(a)(5)(A), a defendant must (among other things) transmit a program onto a computer and thereby cause "damage" to

it—that is, the program must "impair[] the integrity or availability of" the computer "system" or of "data . . . or information" stored on the computer. 18 U.S.C. § 1030(e)(8). Since the commercial remote desktop applications at issue here didn't do that, Knoot's alleged conduct didn't "damage[]" the company computers, and, therefore, doesn't amount to computer fraud.

Hoping to convince this Court otherwise, the Government claims that Knoot's alleged conduct caused two types of "damage" to the company computers. Neither theory has merit.[1]

1. First, the Government submits that Knoot's alleged conduct "impaired the integrity of data and information" on the company computers because it "exposed" that data and information to an "unauthorized individual"—namely, Yang. (DE 80, Gov't Resp., PageID #433).

But as Knoot explained in his opening motion, a person does not "damage" computer information or data within the meaning of the CFAA simply by making it available to a third-party—even if the third-party isn't authorized to view or access it. *See U.S. Gypsum Co. v. Lafarge N. Am. Inc.*, 670 F. Supp. 2d 737, 744 (N.D. Ill. 2009); *see also Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 994 (E.D. Wis. 2010) ("There is virtually no support for the proposition that merely accessing and disseminating information from a protected computer" causes "damage" for computer-fraud purposes.); *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 769 (N.D. Ill. 2009) (reasoning that a program which merely "disclose[s] . . . confidential information" to a third party does not "damage" data, information, a system, or a program).

[1] The Government does not argue that Knoot's alleged conduct "impair[ed]" the "availability" of any data, information, system, or program—instead, it claims only that the conduct impaired the "integrity" of data on the computers and/or the computer "systems themselves." (DE 80, Gov't Resp., PageID #432-436). For this reason, the Government's reliance on *Shahulhameed*—a case where the defendant's conduct rendered computer data and programs inoperable and inaccessible is misplaced. *United States v. Shahulhameed*, 629 F. App'x 685, 688 (6th Cir. 2015) (finding damage where, among other things, the defendant transmitted commands on a computer "which made it impossible for servers to communicate with each other, effectively shutting the servers down").

Notably, the Government makes no effort in its response to distinguish any of the above-cited cases, nor does it point to any facts (in the indictment or otherwise) suggesting that, as a result of Knoot's alleged conduct, data or information stored on the company computers is no longer accurate or reliable. Rather, as Knoot noted in his opening motion, it appears from the indictment that all that happened is that Yang accessed the company computers and performed IT work for the benefit of the companies. To that end, the Government's first "damage" theory fails.

2. Second, the Government suggests that, even if Knoot's alleged conduct did not impair the integrity of any *data* stored on the computers, the conduct nonetheless "impaired the integrity" of the computer "systems themselves." (DE 80, Gov't Resp., PageID #433). As support, the Government theorizes: (1) that Companies A, B, C, and D "put" "security controls" on their computers to prevent them (the computers) from connecting to other computers via "remote desktop protocol[s]," and (2) that, accordingly, Knoot must have "circumvented" those "security controls" when he installed the remote desktop applications. (*Id.*, PageID #433). Because Knoot "circumvented" those "baseline security controls," the Government concludes, he necessarily "impair[ed]" the integrity of the company computers by causing them to operate in a way "that was unintended" by the owners. (*Id.*, PageID #433). This take on "damage" doesn't work.

For starters, nothing in the indictment suggests that Knoot had to (or did in fact) disable any security features on any of the company computers in order to install remote desktop applications on them—hence, it's unclear why the Government believes he "circumvent[ed]" "security controls" that were "put in place" by the companies. (*Id.*, PageID #433).

But even setting that problem aside, the Government's theory essentially boils down to the following proposition: "Where a company" has a policy that prohibits (or, more broadly, a policy that simply does not authorize) the installation of an application on a company computer, the act

of installing that application "damages" the computer because, post-installation, the computer has a feature that the owner did not "[]intend" for it to have. (DE 80, Gov't Resp., PageID #433).

And that cannot be correct. For one thing, this theory seemingly violates the presumption against surplusage by collapsing § 1030(a)(5)(A)'s "transmission" and "damage" requirements into a single element—i.e., if a person is not authorized to *transmit* a program onto a computer, then doing so *damages* the computer.[2] *Gen. Med., P.C. v. Azar*, 963 F.3d 516, 521 (6th Cir. 2020) (discussing the presumption against surplusage). And for another, if accepted, this theory would criminalize "violations of private computer use policies"—or even worse, an employer's subjective (and potentially unwritten) expectations about how a company computer should operate. *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012). Given that courts—including the Supreme Court—have historically refrained from interpreting the CFAA to criminalize workplace misconduct, the Government's position is untenable. *Id.*; *see also Van Buren v. United States*, 593 U.S. 374, 393 (2021) (rejecting government's broad interpretation of CFAA because to accept it "would attach criminal penalties to" the violation of an IT policy).

Seeking a contrary result, the Government suggests that Southern District of New York's decision in *Yücel* lends supports its argument that the unauthorized transmission of a remote desktop application onto a protected computer "alter[s] the [computer's] baseline security configuration" and thereby "cause[s] 'damage'' to it. (DE 80, Gov't Resp., PageID #434-35).

But *Yücel* is not as helpful as the Government suggests. The defendant in that case (Alex Yücel) developed malware under the brand name "Blackshades" and then sold it to customers who

[2] Relatedly, insofar as the Government's theory is that Knoot "damage[d]" or conspired to "damage" the company computers simply by giving Yang access to them, the Government's position conflates "access" with "damage." And "access" and "damage" cannot be synonymous. If they were, then § 1030(a)(5)(A) would be meaningless because § 1030(a)(4) already makes it a crime for a person to access a computer without authorization.

would, in turn, surreptitiously install it onto vulnerable computers.[3] *See United States v. Yücel*, 97 F. Supp. 3d 413, 416 (S.D.N.Y. 2015). "The malware included a remote access tool." *Id.* And, among other things, that tool captured: (1) "the victims' keystrokes as they type[d]" and (2) "scanned victims' hard-drives for" credit card numbers *Id.* That is, the malware "harvest[ed]" (or stole) "financial information" stored on infected computers. *Id.* at 422. Further, as the Government explained in another case involving the Blackshades malware, the malware was often installed in a way that made it "undetectable by anti-virus software." (*See* United States v. Brendan Johnson, 14-MAG-1086, Sealed Complaint, ¶ 19 (S.D.N.Y. May 16, 2014), available here).

Given that background, the Government indicted Yücel for knowingly transmitting a program (namely, the malware) onto protected computers with the intent to cause damage without authorization, in violation of 18 U.S.C. § 1030(a)(5)(A). *Yücel*, 97 F. Supp. at 416.

As the case developed, Yücel moved to dismiss the indictment, arguing that § 1030(a)(5)(A)'s "damage" element was void for vagueness. *Id.* at 421. Specifically, he claimed that courts disagreed about what "constitutes damage" and that the statute's definition of "damage" was so vague that he could not have known that his conduct was unlawful. *Id.* at 421.

But the court denied his motion, reasoning that "'no person of ordinary intelligence could believe that [it was] somehow legal' to install [malware] on the victims' computers without their consent and harvest their financial information." *Id.* at 421 (citation omitted).

Against that backdrop, it's difficult to see how *Yücel* saves the Government's claim or how this case is "analogous," (*see* DE 80, Gov't Resp., PageID #434), to *Yücel*. True (as the Government emphasizes in its response), *Yücel* suggests that § 1030(a)(5)(A)'s "damage" element is met any time a person adds an "unwanted characteristic" to another's computer without

[3] To learn more about the Blackshades malware, see this press release.

permission. *Id.* at 420. But in context, all the court held was that Yücel's act of creating and installing data-harvesting malware onto a computer "damage[d]" it. And the allegations here don't resemble Yücel's conduct in the slightest. For instance, the indictment contains no facts suggesting that Knoot (or anyone else) installed malware on any of the company computers. Nor does it contain any allegations indicating that any sensitive data was corrupted or stolen off of any of those computers. Rather, the Government's claim in this case is that Knoot "damage[d]" the computers simply by setting them up in a way that allowed Yang to logon to them and complete IT work for the companies' benefit. Suffice it to say, this case and *Yücel* are worlds apart.

To that end, and contrary to the Government's theories, the indictment does not adequately allege a violation of § 1030(a)(5)(A). Counts One & Four should be dismissed.

B. <u>Count Five: Aggravated Identity Theft</u>

Count Five is also subject to dismissal for failure to state an offense. The theory behind this count is: (1) that Yang committed the crime of aggravated identity theft in violation of 18 U.S.C. § 1028A when he used A.M.'s stolen identity to apply for and obtain remote IT jobs, and (2) that Knoot is criminally responsible for Yang's conduct because he helped or encouraged the commission of the crime with the intent that the crime be committed. (DE 72, Mot. Dismiss, PageID #416). But as Knoot explained in his opening motion, this theory is untenable for three reasons. Those reasons, and the Government's response to them, are discussed below.

1. First, Knoot argued in his opening motion that the indictment fails to adequately plead that Knoot aided-and-abetted Yang's alleged violation of the aggravated identity theft statute because it doesn't include facts suggesting that Knoot knew that A.M.'s identity had been stolen—much less that he encouraged Yang to steal it or to use it to apply for IT jobs. (*Id.*, PageID #421).

In fact, Knoot noted, the indictment actually undercuts the Government's theory because, per the indictment, it appears that Yang (or someone else) stole A.M.'s identity and used it to secure employment with IT companies *before* he allegedly asked Knoot to facilitate his (Yang's) work for those companies. (*Id.*, PageID #411 (setting out timeline alleged in indictment)).

How could Knoot have "encouraged" or "helped" Yang to steal A.M.'s identity and use it to apply for remote IT jobs if Yang had already completed those actions before Knoot's involvement? Sixth Circuit Pattern Jury Instruction No. 4.01, *Aiding and Abetting*.

In response, the Government points to paragraphs 6-8 of the indictment, claiming that these paragraphs recite facts which (if proven) show that Knoot "was aware at relevant times" that Yang was using A.M.'s stolen identity to secure work. (DE 80, Gov't Resp., PageID #430-440).

But these paragraphs say no such thing. Paragraph 6 says that Knoot "acted as a facilitator for one or more overseas IT workers using the persona YANG DI and conspired with them to obtain their employment with U.S. companies, perform work remotely, share in the proceeds generated by the remote IT work, and launder the proceeds of the scheme." (DE 3, Indictment, PageID #5). Nothing about those factual recitations suggests that Knoot knew that Yang had stolen A.M.'s identity (much less that he "encouraged" Yang to steal it and use it to get work). Further, Paragraphs 7 and 8 say that Yang "used the stolen identity of a U.S. citizen"—namely, A.M.—"to apply for and obtain remote IT work at U.S. companies." (*Id.*, PageID #5). Fair enough, but nothing in this paragraph suggests that Knoot: (1) helped Yang steal someone's identity and used it to obtain remote IT work, or (2) even knew that Yang had done so.

Further, even if the allegations in the indictment *could* be construed as suggesting that Knoot "was aware at relevant times" that Yang had stolen A.M.'s identity (as the Government argues), its aiding-and-abetting theory would still fail because, as the Committee Commentary to

the Sixth Circuit's aiding-and-abetting instruction show, the fact that a person has "[k]knowledge that a crime is being committed" is "not enough to constitute aiding and abetting." Sixth Circuit Pattern Jury Instruction No. 4.01, *Aiding and Abetting* (discussing cases).

In this way, and contrary to what the Government says (DE 80, Gov't Resp., PageID #439), Knoot does not know *why* the Government believes that he helped Yang steal A.M.'s identity or use A.M.'s identity to apply for IT jobs, nor does he know *how* he assisted Yang in carrying-out those tasks. As such, the indictment fails to plead facts sufficient to state a claim that Knoot aided-and-abetting Yang's violation of the aggravated-identity-theft statute. Dismissal is warranted.

2. Second, and setting the aiding-and-abetting allegations aside, Knoot also argued that Yang didn't commit aggravated identity theft (such that Knoot could not have aided the commission of that offense) because the use of A.M.'s identity was not the but-for cause of what made the underlying scheme illegal or successful. (DE 76, Mot. Dismiss, PageID #417-419).

As support, he relied on the Supreme Court's decision in *Dubin*—a case in which the Court held that the aggravated-identity-theft statute only applies when a person's illegal use of another's means of identification is (at the very least) the but-for cause of what makes a broader felonious scheme successful and illegal (*Id.* (discussing *Dubin v. United States*, 599 U.S. 110, 116 (2023)).

And since the Government's computer-and-wire-fraud theory would be equally applicable if Knoot had secured the IT jobs in question and then farmed the work out to Yang via a remote desktop application, Knoot concluded, A.M.'s identity wasn't necessary to the alleged scheme—that is, the identity wasn't using "during and in relation to" the alleged computer and wire frauds.

In response, the Government seemingly agrees that Yang didn't need A.M.'s identity to carry out the alleged computer-and-wire-fraud scheme—instead, the Government acknowledges, Yang just needed the identity of a "U.S. person." (DE 80, Gov't Resp., PageID #439).

But that's exactly why the use of A.M.'s identity did not cause the success (or alleged illegality) of the underlying scheme. Consider: If Knoot had secured an IT job with Company A, installed a remote desktop application on Company A's laptop, and then allowed Yang to access Company A's computer and perform work for Company A's benefit, the Government would still be claiming that he and Yang conspired to commit computer fraud (on the theory that Knoot damaged the computer "system") and wire fraud (on the theory that the companies paid Knoot under the false pretense that Knoot, rather than Yang, was doing the work).

The upshot? A.M.'s identity was not necessary to the commission of the alleged scheme, and, therefore, the use of his identity was not at the "crux of what" made the underlying "conduct criminal." *Dubin*, 599 U.S. at 131. And that being the case, A.M.'s identity wasn't used "during and in relation to" the underlying computer-and-wire frauds. This count should be dismissed.[4]

3. Third, Knoot argued that, should the Court have doubts about whether the use of A.M.'s identity was at the "crux" of what made the underlying scheme illegal—that is, if it's simply too difficult to determine "the extent to which" A.M.'s identification "'caused'" the predicate offenses or underlying scheme, *see id.* at 135 (Gorsuch, J., concurring)—then the Court should follow Justice Gorsuch's lead and rule that the aggravated-identity-theft statute is void-for-vagueness, at least as applied in this case. (DE 76, Mot. Dismiss, PageID #419-20).

In response, the Government simply points out that Justice Gorsuch's *Dubin* concurrence "is not controlling law" and that the majority in *Dubin* concluded that the aggravated-identity-theft statute is *not* void-for-vagueness. (DE 80, Gov't Resp., PageID #439). True enough. But this case highlights the problems with *Dubin*'s test, and, more broadly, with the aggravated-identity-

[4] The Government suggests that whether Yang used A.M.'s identity "during and in relation to" the underlying computer-and-wire frauds is a question for the jury, but Knoot respectfully disagrees. The parties appear to agree that the alleged scheme could've been carried out the exact same way without the use of a stolen identity. That being the case, the use of A.M.'s identity cannot be the "but-for" cause of the scheme's success.

theft statute. Accordingly, counsel raised a vagueness challenge (adopting the reasoning of Justice Gorsuch's concurrence) in order to preserve it for appellate review (should appeal be necessary).

In sum, the aggravated-identity-theft count should be dismissed. The Government's aiding-and-abetting theory is a non-starter because it failed to plead facts in the indictment establishing that Knoot helped Yang steal or use A.M.'s identity to obtain IT jobs—in fact, the timeline articulated in the indictment suggests that Yang used A.M.'s stolen identity to obtain IT jobs *before* Knoot's alleged involvement in the underlying crimes. And even beyond that, no one committed aggravated identity theft in this case because the use of A.M.'s identity was not at the crux of what made the alleged scheme successful or illegal. Dismissal is warranted.

C. Count Six: Conspiracy to Unlawfully Employ an Unauthorized Alien

Last, the Government claims that Knoot conspired to "hire," "recruit" or "refer" Yang (an unauthorized alien) for employment in violation of 8 U.S.C. § 1324a(a)(1)(A) when he "allow[ed] Yang . . . to obtain remote work using [his] physical and Internet Protocol Addresses." (DE 80, Gov't Resp., PageID #440-41). In other words, according to the Government, because Knoot allegedly put Yang in a position to perform work for Companies A, B, C, and D, Knoot conspired to "hire," "recruit," or "refer" Yang for employment with those companies. (*Id.*).

That theory doesn't cut it. Section 1324a(a)(1)(A) makes it illegal for a person or entity to "hire," "recruit," or "refer" an unauthorized alien "for employment." As a matter of text, a person "hire[s]" an alien "for employment" when he "pay[s]" the alien "for labor or personal services" as part of an employer-employee relationship. *See* Merriam-Webster Online Dictionary, *Hire*, available here. Likewise, a person "recruit[s]" or "refer[s]" an alien for employment" when the person "seek[s]" employment on behalf of an alien or recommends an alien for employment. Merriam-Webster Online Dictionary, *Recruit* and *Refer* available here and here. Given these

definitions, and even assuming Knoot conspired to "allow" Yang to use his "physical and Internet Protocol Addresses" to complete work for the companies, that conduct does not give rise to a conspiracy to "hire," "recruit," or "refer" Yang for employment with those companies.

Further, and contrary to the Government's suggestion, § 1324a(a)(1)(A) only subjects employers and staffing agencies (i.e., the types of "person[s]" or "entities" who "hire," "recruit," and "refer" others for employment) to criminal liability. This is evident from the fact that the Supreme Court has always discussed this statute in the context of employer-employee relationships, *see, e.g.*, *Hoffman Plastic Compounds, Inc. v. N.L.R.B.*, 535 U.S. 137, 141 (2002), and the fact that exhaustive Westlaw research failed to turn-up a single case (published or otherwise) involving a situation where a person was convicted of "conspiring" to hire, recruit, or refer an alien for employment simply for putting an alien in a position to complete work.

Consequently, Knoot did not conspire with anyone to "hire," "recruit," or "refer" Yang for employment—indeed, under the Government's own theory, all Knoot did was help Yang complete work. Because helping an illegal alien complete a job he has been hired to complete is not the same thing as hiring, recruiting, or referring the alien for employment (or conspiring to do the same), the Government's theory fails as a matter of law. This count should be dismissed.

CONCLUSION

In light of the foregoing, Knoot respectfully asks this Court to grant his Motion to Dismiss (DE 76) and to dismiss with prejudice Counts 1, 4, 5, and 6 of the indictment.

Respectfully submitted

/s/ *David K. Fletcher*
DAVID K. FLETCHER
Assistant Federal Public Defender
810 Broadway, Suite 200
Nashville, TN 37203
615-736-5047
E-mail: David_Fletcher@fd.org

Attorney for Matthew Isaac Knoot

CERTIFICATE OF SERVICE

I hereby certify that on July 21, 2025, I electronically filed the foregoing *Reply Supporting Motion to Dismiss* with the U.S. District Court Clerk by using the CM/ECF system, which will send a Notice of Electronic Filing to the following: Joshua A. Kurtzman, Assistant United States Attorney, 719 Church Street, Suite 3300, Nashville, Tennessee, 37203 and Gregory Jon Nicosia, Jr., U.S. Department of Justice-National Security Division, 950 Pennsylvania Avenue, N.W., Washington, DC 20530.

/s/ *David K. Fletcher*
DAVID K. FLETCHER